

[Home](#)
[Operating Systems](#)
[Windows](#)

1. [Introduction](#)
2. [Windows 2000 Professional](#)
3. [Windows 2000 Server](#)
4. [Windows 2000 Advanced Server](#)
5. [Windows 2000 Datacenter Server](#)
6. [Application Support](#)
7. [System Operation](#)
8. [Disks and Volumes](#)
9. [Filesystems](#)
10. [Configuration Files](#)
11. [Security](#)
12. [Network Support](#)
13. [Access Management](#)
14. [Processes](#)
15. [AD Structure](#)
16. [AD Objects](#)
17. [AD Object Naming](#)
18. [AD Schema](#)
19. [AD Sites](#)
20. [Domains](#)
21. [AD Functions](#)
22. [AD Replication](#)
23. [DNS](#)

[Previous Page](#) | [Next Page](#)

Save Yourself Some Frustration - Learn:

[Why You Need a Firewall](#) [Why Spyware and Adware are Dangerous](#)

[How You Can Change System Settings to Help Prevent Spyware](#)

Windows 2000 Authentication

Authentication is performed by the system to be sure the user is really who they claim to be. Authentication may be done at and for a local computer or at a global level for a domain using domain controllers across the network. Windows 2000 supports the following types of authentication:

- **Kerberos V5 (RFC 1510)** - An Internet standard authentication protocol which is the default protocol for Windows 2000 computers within a domain. This is not used for computers in different forests.
- **Windows NT LAN Manager (NTLM)** - Used to authenticate users from Windows 95, 98, and NT systems. Windows 2000 Active Directory must be operating in mixed mode to use this authentication method.
- **Secure Sockets Layer/Transport Layer Security (SSL/TLS)** - Requires certificate servers and is used to authenticate users that are logging onto secure web sites.
- **Smart card** - Contains a chip with information about the user along with the user's private key. A personal identification number (PIN) is normally required to be authenticated using a smart card. Requires Extensible Authentication Protocol (EAP) to be enabled for the server to allow smart card authentication. Also some certificate authority must provide keys.

Authentication uses X.509 standard and Kerberos.

Process of Logging On

1. CTRL+ALT+DEL is pressed, name and password entered, and local or domain logon is indicated.
2. If the logon is local, the name and password are checked against the local database. If the logon is a domain logon, the name and password are encrypted into a key, and timestamp information is encrypted. This information is sent to the Windows 2000 domain controller with an authentication request.
3. The domain controller decrypts the information and checks for a valid timestamp. If the timestamp is valid, two Kerberos tickets are made and encrypted with the password. The tickets are sent back to the client computer. The tickets are:
 - User session key - Used to log on.
 - User ticket - Used to get other Kerberos tickets for accessing other domain resources.
4. The client decrypts the tickets and uses the session key to log on.

Authentication when Accessing an Object

1. The user tries to access the network object.
2. The user ticket, user name, name of the object to access, and timestamp, are sent with a Kerberos ticket granting service request to the domain controller.

Ads by Google

Two Factor Authentication
 eSprint - authentication solution for online banking.
 Hardware-free.
www.crsd.com/esprint

Two-Factor Authentication
 No tokens, no software to deploy. Proven process to thwart ID Theft.
www.auditonly.com

Competitive Token Upgrade
 Next generation two-factor authentication for under \$10 TCO.
www.verisign.com

Two-Factor Authentication
 Use telephones for authentication. No additional hardware required.
www.1stcym.com

Exhibit A

24. AD Security
25. AD Installation
26. AD Configuration
27. AD Performance
28. Installation
29. Installation Options
30. Unattended Installation
31. Software Distribution
32. Ranale Installation Service
33. Language
34. Accessibility
35. File Attributes
36. Shares
37. Distributed File System
38. Control Panel
39. Active Directory Tools
40. Computer Management
41. Console Tools
42. MMC Tools
43. Network Monitor
44. System Performance Monitoring
45. Tools
46. Managing Services
47. Connections
48. TCP/IP
49. DHCP
50. Printing

Shares used for logon

NETLOGON\SYSVOL - The Netlogon share is used on Windows NT domain controllers to authenticate users. In Windows 2000, the SYSVOL share carries out these functions. The SYSVOL share includes group policy information which is replicated to all local domain controllers.

Free Technical Resources at JMRTechnical.com

PHP Tutorials MySQL Cisco Antivirus Tips
Windows 2000/XP Linux Technical Links Adware Tips

Authentication

- 51. Rawling
- 52. IPSec
- 53. ICS
- 54. Fault
- Tolerance
- 55. Backup
- 56. System Failure
- 57. Services
- 58. Remote
- Access
- 59. WINS
- 60. IS
- 61. Certificate
- Server
- 62. Terminal
- Services
- 63. Web Services
- 64. Authentication
- 65. Accounts
- 66. Permissions
- 67. Groups
- 68. User Rights
- and Auditing
- 69. Auditing
- 70. User Profiles
- 71. Policies
- 72. Group Policies
- 73. Miscellaneous
- 74. Terms
- 75. Credits
- Windows
- Operating Systems
- Home